SOLUTION BRIEF

Reduce Ransomware Risk With the Fortinet Security Fabric

Utilizing a Cybersecurity Mesh Architecture

Executive Summary

Today's organizations have a broad digital attack surface spanning a diverse set of devices, user locations, networks, and clouds, providing many avenues of entry and exfiltration for cybercriminals. Increasingly, these cybercriminals are doing more than stealing data, often encrypting whole systems and interrupting business operations with ransomware, a threat that's increased 15x over the past 18 months.

The Fortinet Security Fabric is a cybersecurity platform that covers the entirety of an organization's attack surface with independently validated prevention, along with tightly integrated detection for all stages of the cyber kill chain and automated response capabilities. A range of services from FortiGuard Labs augment in-house security expertise to prepare, practice, and monitor for ransomware and recover from it as needed.

Reduce Ransomware Risk With Fortinet

Preparation

Fortinet offers a range of services to help organizations prepare for attempted intrusion by ransomware operators and their payloads. Organizations can take advantage of FortiGuard experts to help them assess their ransomware readiness, define policies, implement playbooks, and conduct tabletop exercises. This is all part of the FortiGuard Incident Readiness Service and can be complemented by the automated testing of FortiTester and FortiPentest, as well as end-user education with the Fortinet Security Awareness and Training Service.

Prevention

The Fortinet Security Fabric includes best-of-breed endpoint, email, network, web application, and cloud security controls that provide consistently top-rated threat prevention capabilities to reduce the risk of ransomware actors and components gaining entry to any organization.

FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyberthreats, including those that are used by cybercriminals to insert ransomware with a range of advanced technologies like content disarm and reconstruction, sandbox analysis, and browser isolation. FortiGate enterprise firewalls consolidate industry-leading security capabilities, such as secure sockets layer (SSL) inspection, including the latest TLS 1.3, web filtering, and intrusion prevention system (IPS) to provide full visibility and protect all network edges.

FortiWeb protects the applications on which organizations depend with machine learning–based web application security. FortiEDR provides modern, behavior-based endpoint security (including patented ransomware protection) for the devices on which applications run and/or users depend.

Detection

All of these products are powered by security subscriptions from FortiGuard Labs and integrate with the dedicated, advanced threat protection of FortiSandbox and FortiAI to reduce the risk of ransomware components being successfully delivered via email or the web.

That said, organizations need not wait for the delivery stage of the cyber kill chain to detect cybercriminal activity. FortiDeceptor deploys dedicated infrastructure specifically designed to attract the attention of cybercriminals and provide early warning of initial reconnaissance or compromised systems. At the same time, FortiRecon can uncover weaponized infrastructure that is often prepared in advance of upcoming, targeted ransomware attacks.

However, just in case a ransomware operator or component reaches an endpoint, the integrated endpoint detection and response (EDR) components of FortiEDR can provide patented "detect and defuse" capability as well as the automation for fast response. The FortiInsight module can also be enabled on the same endpoints to monitor user behavior for insider risk.

This is a critical security analytics and threat intelligence layer that facilitates fast response to incidents in progress.

78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more. Having too many security vendors results in complex security operations and increased security headcount.[1]

Monitoring and response

While the artificial intelligence (AI) embedded in the detection products above is a major assist to security staff, human oversight and final response are recommended.

Fortinet offers a range of security operations center (SOC) platform components, starting with the foundational Fabric visibility, analytics, and automation framework of FortiAnalyzer and the fully automated add-on of FortiXDR. For larger or more mature security operations, FortiSIEM adds multivendor visibility and analytics, while FortiSOAR supports orchestration and automation of defined security processes—all of which speed response from efficient security operations.

FortiGuard Managed Detection and Response Service handles FortiEDR alerts and incidents. At the same time, the FortiGuard team also provides staff augmentation services, including SOC-as-a-Service for organizations seeking assistance with firewall triage and other alerts received by FortiAnalyzer. Finally, the expert Incident Response Service assists in-house security teams, should organizations find themselves amid a major cybersecurity incident.

The Fortinet Difference

The Fortinet Security Fabric and supporting services help organizations with almost any aspect of securing against cybercriminals and ransomware campaigns. Whether it's people services to prepare for or respond to ransomware incidents or products and services to better prevent, detect, and contain potential incidents, Fortinet helps organizations reduce the risk and potential impact of increasingly common and sophisticated ransomware.

Further, tight integration and automation of the platform products and services ensure that as organizations add more Fortinet elements over time, they reduce cyber risk and the burden on their security teams.

Whether it's securing a new edge of the attack surface, strengthening protection for an existing one, deploying detection for additional kill-chain stages, improving the security monitoring function, or augmenting existing teams with specialized experts, organizations can rely on a trusted security partner in Fortinet.

Conclusion

The risk of ransomware is real and growing due to the multistage sophistication of many campaigns. However, that same sophistication can be used against cybercriminals as the multiple stages provide multiple opportunities for detection and response before their end objectives can be achieved. But only if the organization properly prepares and puts the right technologies in place across the organization's attack surface and along the kill chain and has the staff and skills necessary to recognize and contain incidents in progress.

That's why Fortinet has built the broad, integrated, and automated Security Fabric, with supporting SOC services, in alignment with one of Gartner's Strategic Technologies for 2022, the Cybersecurity Mesh Architecture.

[1] "The Top 8 Security and Risk Trends We're Watching," Gartner, November 15, 2021.

March 3, 2022 12:06 PM
1469355-0-0-EN